BI.ZONE

# BI.ZONE Brand Protection

## Как мошенники похищали домены и маскировали их под фишинговые сайты

Дмитрий Кирюшкин

Руководитель отдела анализа репутации

BI.ZONE

# Статистика BI.ZONE Brand Protection *

**925**

утечек баз данных
проанализировано
за 2022 год

**110 тыс.**

фишинговых ресурсов
заблокировали специалисты
BI.ZONE в 2022 году

**10 пар**

«корпоративная почта +
пароль» на каждые
100 сотрудников в утекших
базах данных

**70%**

вероятность найти фишинговый
сайт на компанию,
если у ее пользователей
есть личные кабинеты

*По данным BI.ZONE

BI.ZONE

# С чем мы столкнулись

## Дано

Поступили многочисленные обращения от владельцев доменов из различных отраслей: от интернет-магазинов до учебных порталов. Владельцы хотели узнать причину блокировки их доменов

## Анализ

Преступники с начала 2023 года похитили более 600 ресурсов и размещали фишинговый контент, пользуясь мисконфигурацией NS-записей

BI.ZONE

# Что такое угон домена

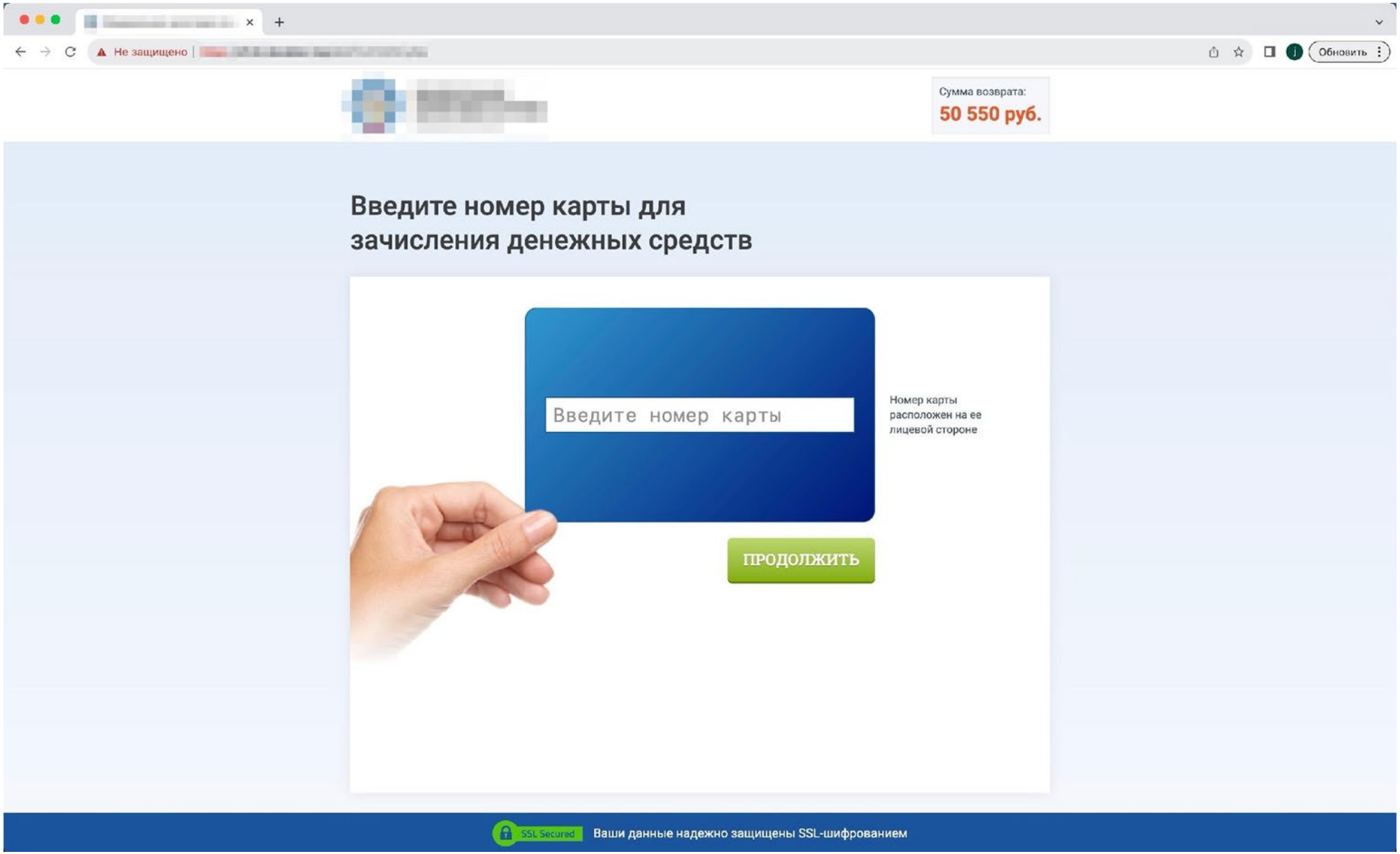
Пользователь покупает домен
и забывает про его существование

Злоумышленник находит неправильно
сконфигурированный домен и размещает там
фишинговый контент

Домен блокируется, а его владелец
обращается к нам с просьбой объяснить,
почему его старый домен, с которым он
ничего не делал, был заблокирован

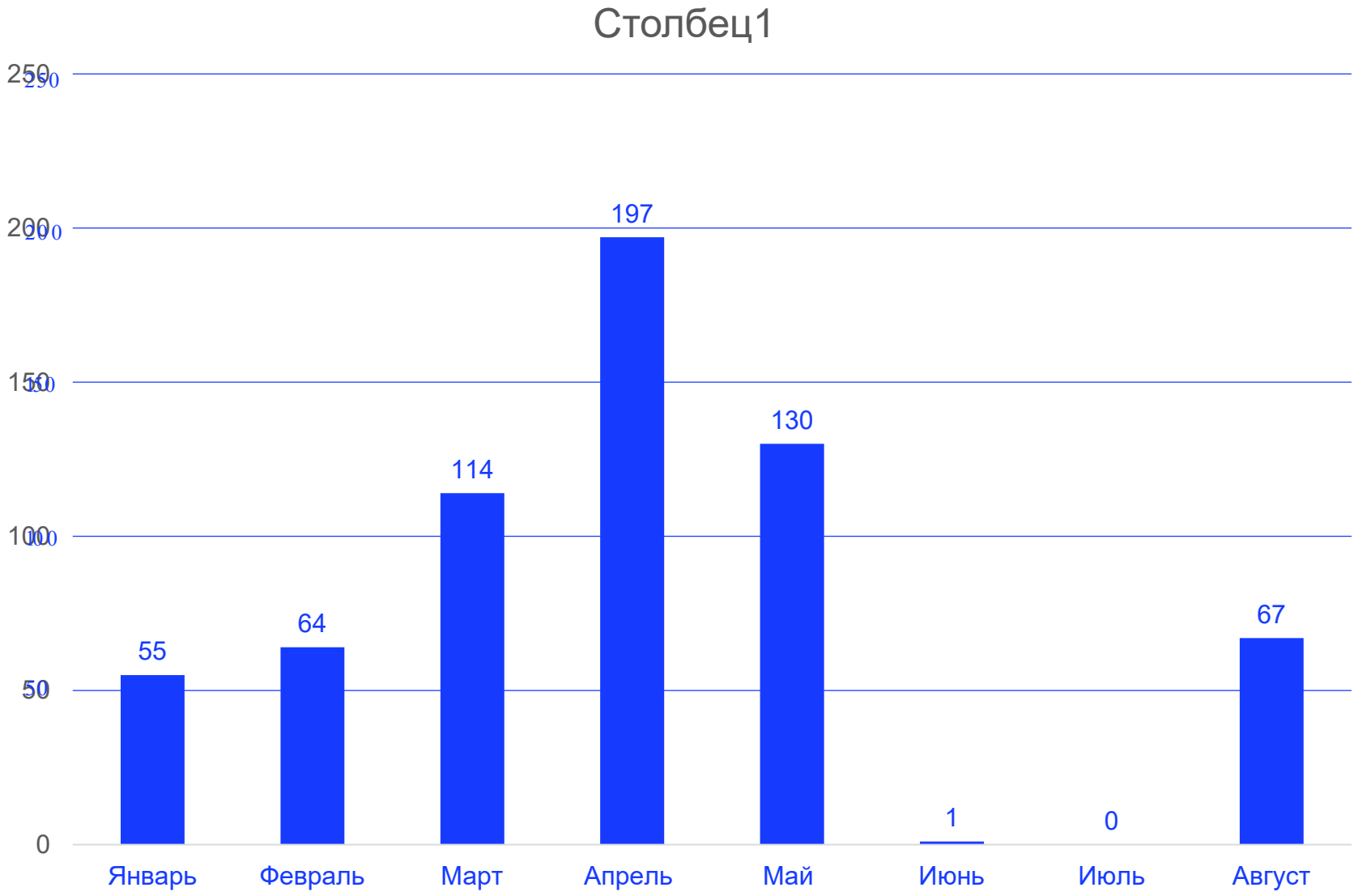
BI.ZONE

# Пример угнанного домена



BI.ZONE

# Угнанные домены в 2023 году*




*По данным BI.ZONE

BI.ZONE

# Рекомендации

01

Полностью удаляйте текущие NS-записи (связывающие доменное имя с DNS-сервером) в личном кабинете регистратора доменного имени, если срок оплаты заканчивается и вы не планируете его продлевать

02

Не прописывайте в личном кабинете регистратора NS-записи хостинг-провайдера до привязки самого домена к хостинг-аккаунту

BI.ZONE

ул. Ольховская, д. 4, корп. 2
г. Москва, 105066
+7 499 110-25-34
info@bi.zone